eSecurity

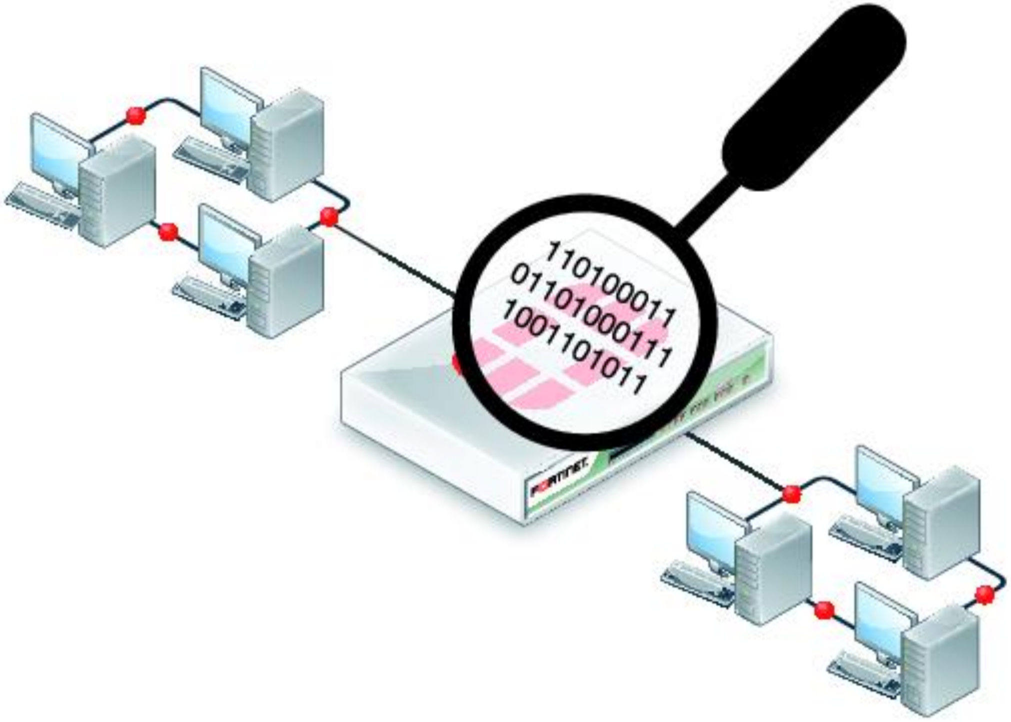
Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Auditoria de Senhas:**
  - ✓ Sniffing
  - ✓ Wireshark
    - ✓ Conceito
    - ✓ Filtros
  - ✓ O protocolo FTP
  - ✓ O protocolo POP3

Auditoria Passiva de Senhas



Sniffing

Sniffing, a um grosso modo, seria você ficar com os ouvidos atentos para ouvir qualquer coisa que seja dita ao seu alcance.

Atualmente, quase todos os ambientes utilizam switches e não mais hubs, o que torna o *sniffing* um POUCO mais difícil, pois os switches não enviam os dados para todas as portas como um hub faz, ele envia diretamente para a porta onde se encontra o host de destino; então, se você tentar “sniffar” uma rede com switch você irá apenas ouvir o que for *broadcast*, ou sua própria conexão.

Para conseguir ouvir tudo sem ser o gateway da rede, é necessário um ataque de arp spoof, ou estourar a tabela CAM do switch.

Wireshark: Conceito

O Wireshark é uma ferramenta muito poderosa que vai muito além de um simples sniffer. O que muitos não sabem é que existem várias formas de se aproveitar o potencial desta ferramenta, mas nesta aula iremos iniciar do básico. Vamos aprender a sniffar a rede de forma efetiva, criar filtros para buscar apenas a informação que queremos.

Veremos como um pentester/auditor utilizaria esta ferramenta para roubar senhas e para finalizar o teste de intrusão, como utilizar o Wireshark para diagnosticar problemas de rede ou se um firewall está bloqueando os pacotes corretamente.

Wireshark: Filtros

Segue uma lista dos principais filtros utilizados no Wireshark:

FILTRO	EXPLICAÇÃO	EXEMPLO
ip.addr	endereço IPv4 de destinou ou origem	ip.addr == 10.10.10.10
ip.dst	endereço de destino IPv4	ip.addr == 10.10.10.10
ip.src	endereço de origem IPv4	ip.src == 10.10.10.10
ip.proto	Protocolo IP (decimal)	ip.proto == 1
ipv6.addr	endereço IPv6 de origem ou destino	ipv6.addr == 2001 :: 5
ipv6.src	endereço IPv6 de origem	ipv6.addr == 2001 :: 5
ipv6.dst	endereço de destino IPv6	ipv6.dst == 2001 :: 5
tcp.port	porta TCP de destino ou origem	tcp.port == 20
tcp.dstport	porta TCP de destino	tcp.dstport == 80
tcp.srcport	porta TCP de origem	tcp.srcport == 60234
udp.port	porta UDP de destino ou origem	udp.port == 513
udp.dstport	porta UDP de destino	udp.dstport == 513
udp.srcport	porta UDP de origem	udp.srcport == 40000
icmp.type	Código do tipo ICMP (decimal)	icmp.type == 8

* Você pode definir vários itens com a opção &&

O protocolo FTP:

FTP ou File Transfer Protocol (em português, Protocolo de Transferência de Arquivos), é uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet.

Pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo (Servidor FTP, neste caso, tradicionalmente aparece em letras minúsculas, por influência do programa de transferência de arquivos do Unix).

Um cliente realiza uma conexão TCP para a porta 21 do servidor. Essa conexão, chamada de conexão de controle, permanece aberta ao longo da sessão enquanto uma segunda conexão, chamada conexão de dados, é estabelecida na porta 20 do servidor e em alguma porta do cliente (estabelecida no diálogo entre ambos) como requisitado para a transferência de arquivo. A conexão de controle é utilizada para administração da sessão (comandos, identificação, senhas) entre cliente e servidor utilizando um protocolo semelhante ao Telnet.

Fonte: Wiki

O protocolo POP3:

O Post Office Protocol, ou POP3, é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. Permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local.

O funcionamento do protocolo POP3 diz-se off-line, uma vez que o processo suportado se baseia nas seguintes etapas:

- É estabelecida uma ligação TCP entre a aplicação cliente de e-mail (User Agent - UA) e o servidor onde está a caixa de correio (Message Transfer Agent - MTA)
- O utilizador autentica-se;
- Todas as mensagens existentes na caixa de correio são transferidas sequencialmente para o computador local;
- As mensagens são apagadas da caixa de correio (opcionalmente, o protocolo pode ser configurado para que as mensagens não sejam apagadas da caixa de correio; se esta opção não for utilizada, deve-se utilizar sempre o mesmo computador para ler o correio eletrônico, para poder manter um arquivo das mensagens);
- A ligação com o servidor é terminada;
- O utilizador pode agora ler e processar as suas mensagens (off-line).

Fonte: Wiki

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker